AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1 - 21 (Canceled).

Claim 22 (New): A system for maintaining trust in the content of a digital image file, comprising:

a trusted time source to provide a certifiable time for an unalterable time stamp, wherein said certifiable time confirms at least one of said digital image file's access, creation, modification, receipt, or transmission;

means for receiving said request to save said digital image file from a user;

first means for saving said digital image file at a moment in time;

means for retrieving from said trusted time source a date and a time corresponding to said moment in time, wherein said moment in time is substantially the current time of said trusted time source corresponding to receipt of said request;

first means for appending said date and said time retrieved from said trusted time source to said digital image file;

first means for signing said digital image file with said date and said time retrieved from said trusted time source appended thereto;

means for hashing said digital image file to produce a digest;

second means for signing said digest with a key to produce a certificate;

second means for appending said certificate to said digital image file;

second means for saving said digital image file with said certificate appended thereto;

means for modifying said digital image file with said certificate appended thereto into a modified digital image file, wherein said modifying includes at least one of converting or enhancing;

third means for appending said digital image file with said certificate appended thereto to said modified digital image file; and

means for verifying trust in the content of said digital image file with said certificate appended thereto.

Claim 23 (New): The system of claim 22, further comprising:

second means for receiving a second request to save said modified digital image file from said user;

third means for saving said modified digital image file at a second moment in time;

second means for retrieving from said trusted time source a second date and a second time corresponding to said second moment in time, wherein said second moment in time is substantially the current time of said trusted time source corresponding to receipt of said second request;

third means for appending said second date and said second time retrieved from said trusted time source to said modified digital image file;

third means for signing said modified digital image file with said second date and said second time retrieved from said trusted time source appended thereto;

second means for hashing said modified digital image file to produce a second digest;

fourth means for signing said second digest with a second key to produce a second certificate;

fourth means for appending said second certificate to said modified digital image file;

fourth means for saving said modified digital image file with said second certificate appended thereto; and

second means for verifying trust in the content of said modified digital image file with said second certificate appended thereto.

Claim 24 (New): The system of claim 23, wherein said modified digital image file with said second certificate appended thereto includes said digital image file with said certificate appended thereto.

Claim 25 (New): The system of claim 22, wherein said verification means includes a third means for signing said digital image file with said date and said time retrieved from said trusted time source appended thereto with an identifier.

Claim 26 (New): The system of claim 25, wherein said identifier corresponds to said user and is elected from the group consisting of a platform identifier, a server node identifier, and a network identifier.

Claim 27 (New): The system of claim 25, wherein said identifier is selected from the group consisting of an identifier corresponding to said user, an identifier corresponding to a system used by said user, and an identifier corresponding to an enterprise within which said user uses said computing means.

Claim 28 (New): The system of claim 25, wherein said user identifier is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

Claim 29 (New): The system of claim 22, wherein said trusted time source includes a tamper-evident means.

Claim 30 (New): A method for maintaining trust in the content of a digital image file, comprising:

providing, with a trusted time source, a certifiable time for an unalterable time stamp, wherein said certifiable time confirms at least one of said digital image file's access, creation, modification, receipt, or transmission;

receiving said request to save said digital image file from a user;

saving said digital image file at a moment in time;

retrieving from said trusted time source a date and a time corresponding to said moment in time, wherein said moment in time is substantially the current time of said trusted time source corresponding to receipt of said request;

appending said date and said time retrieved from said trusted time source to said digital image file;

signing said digital image file with said date and said time retrieved from said trusted time source appended thereto;

hashing said digital image file to produce a digest;

signing said digest with a key to produce a certificate;

appending said certificate to said digital image file;

saving said digital image file with said certificate appended thereto; and

verifying trust in the content of said digital image file with said certificate appended thereto.

Claim 31 (New): The method of claim 30, further comprising:

receiving a second request to save said modified digital image file from said user;

saving said modified digital image file at a second moment in time;

retrieving from said trusted time source a second date and a second time corresponding to said second moment in time, wherein said second moment in time is substantially the current time of said trusted time source corresponding to receipt of said second request;

appending said second date and said second time retrieved from said trusted time source to said modified digital image file;

signing said modified digital image file with said second date and said second time retrieved from said trusted time source appended thereto;

hashing said modified digital image file to produce a second digest;

signing said second digest with a second key to produce a second certificate;

appending said second certificate to said modified digital image file;

saving said modified digital image file with said second certificate appended thereto; and

verifying trust in the content of said modified digital image file with said second certificate appended thereto.

Claim 32 (New): The method of claim 30, wherein said modified digital image file with said second certificate appended thereto includes said digital image file with said certificate appended thereto.

Claim 33 (New): The method of claim 30, wherein said verification includes signing said digital image file with said date and said time retrieved from said trusted time source appended thereto with an identifier.

Claim 34 (New): The method of claim 33, wherein said identifier corresponds to said user and is elected from the group consisting of a platform identifier, a server node identifier, and a network identifier.

Claim 35 (New): The method of claim 33, wherein said identifier is selected from the group consisting of an identifier corresponding to said user, an identifier corresponding to a system used by said user, and an identifier corresponding to an enterprise within which said user uses the computing means.

Claim 36 (New): The method of claim 33, wherein said user identifier is selected from the group consisting of a plurality of characters identifying said user, first data representing an iris scan of said

user, second data representing a retina scan of said user, third data representing a finger scan of said user, fourth data representing said user's hand geometry, fifth data representing said user's voice, sixth data representing said user's signature, and combinations of said plurality of characters, first, second, third, fourth, fifth, and sixth data.

Claim 37 (New): The method of claim 30, wherein said trusted time source includes tamper-evident protection.